(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 104 960 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
06.06.2001 Bulletin 2001/23

(51) Int Cl.[7]: **H04L 9/32**, H04L 29/06

(21) Application number: **99124150.6**

(22) Date of filing: **02.12.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **Sony International (Europe) GmbH**
50829 Köln (DE)

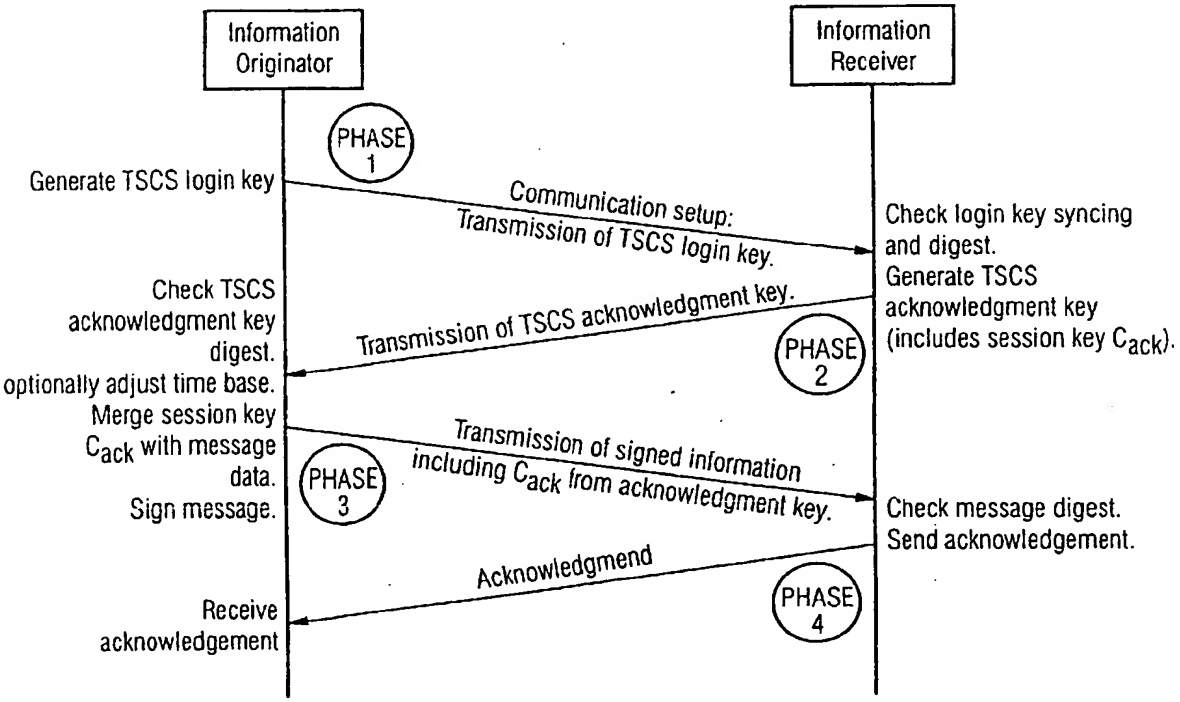
(72) Inventor: **Mache, Niels, Sony Int.(Europe) GmbH**
70736 Fellbach (DE)

(74) Representative: **Rupp, Christian, Dipl.Phys. et al**
Mitscherlich & Partner
Patent- und Rechtsanwälte
Sonnenstrasse 33
80331 München (DE)

(54) Message authentication

(57) For the authentication of messages communicated in a distributed system from an originator to a destination a keyed-hashing technique is used according to which data to be authenticated is concatenated with a private (secret) key and then processed to the cryptographic hash function. The data are transmitted together with the digest of the hash function from the originator to the destination. The data comprises temporal validity information representing the temporal validity of the data. For example the setup key of a communication is therefore only valid within a given time interval that is dynamically defined by the communication originator. After the time interval is exceeded the setup key is invalid and cannot be reused again.

FIG 1



EP 1 104 960 A1

Description

[0001] The present invention relates to a method for the authentication of data communicated from an originator to a destination, to a method for the authenticated transmission of messages, to a software program product capable of implementing such a method, to a distributed system for communicating authenticated data from an originator to a destination as well as to a distributed system for the authenticated transmission of messages.

[0002] Generally the present invention relates to the field of secure communication setup systems and methods which allow the secure communication setup between two communication parties, an originator and a destination. In an authenticated (but not secret) two party communication setup the communication partners and the messages exchange must be authenticated meaning that the communicating parties can verify that the received messages have not been altered as well as that the sender and receiver are authentic.

[0003] Generally there are the following four important aspects of secure communication setup between two communicating parties:

- Assurance that the originating communication partner is authorised to establish the connection (source is authentic),
- assurance that the receiving communication partner is authorised (destination is authentic),
- assurance that the received message was sent by the originating communication partner, and
- assurance that the sent and received message has not been altered.

[0004] From the state of the art it is known to use keyed-hashing message authentication techniques. General background information on message authentication codes (MAC) and cryptographic (one-way) hashing can be found for example in Schneyer, Bruce "Applied Cryptography", Edison-Wessley 1996.

[0005] Keyed-hashing for message authentication (HMAC) is a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, e.g. MD5, SH-1 in combination with a secret (private) shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function. HMAC uses a secret key for calculation and verification of the message authentication values.

[0006] Further information on HMAC can be found for example in Bellare et al "Keying hash functions for message authentication", Proceedings of Crpyto-96, LNCS 1109, pages 1 to 15.

[0007] The very first and initial communication step in communication setup (e.g. the login procedure) is susceptible to copy or replay attacks which send a copy of communication setup (e.g. a user name and password recorded from a login procedure) to the communication partner. This problem is usually solved with additional knowledge about the communication partner at the other side and/or using large random session keys or transaction keys (usually taken from a transaction hearing).

[0008] It is the object of the present invention to provide for a technique reducing the risk of copy or replay attacks particularly in the first step of a communication setup in a more efficient way.

[0009] This object is achieved by means of the features of the independent claims. The dependent claims develop further the central idea of the invention.

[0010] According to the present invention therefore a method for the authentication of data communicated from an originator to a destination is provided. A keyed-hashing technique is used according to which data to be authenticated is concatenated with a private key and then processed with a cryptographic hash function. The data are then transmitted together with the digest of the hash function from the originator to the destination. The data comprise temporal validity information representing the limited temporal validity of the data.

[0011] The temporal validity information can be defined by the originator.

[0012] The data can comprise random data which are unique for a time span defined by the temporal validity information.

[0013] The data can be a login key for a communication setup and/or a message.

[0014] According to another aspect of the present invention a method for the authenticated transmission of messages is provided. A login key is at first generated by a keyed-hashing method on the basis of random data, temporal validity information and a private key. The login key is transmitted from an originator to a destination. The authenticity and the temporal validity of the login key is verified on the basis of the keyed-hashing digest on the destination side.

[0015] In case the verification of the authenticity and the temporal validity of the login key is positive, further acknowledgement steps can be effected. An acknowledgement key can be generated by a keyed-hashing method on the basis of second random data and the private key. The acknowledgement key is transmitted from the destination to the originator. The acknowledgement key is then verified by the originator.

[0016] The acknowledgement key can furthermore comprise a time stamp and when verifying the acknowledgement key it can be checked on the basis of the time stamp and the temporal validity information whether the acknowledgement key is still valid.

[0017] The method can furthermore comprise message transmission steps in case the verification of the acknowledgement key is positive. The second random data of the acknowledgement key are extracted. A message is generated by a key hashing method on the basis of the second random data, message data and the private key. The message is then transmitted from the originator to the destination and the message is verified by

the destination.

[0018] The message can furthermore comprise a time stamp and when verifying the message it is checked on the basis of the time stamp and the temporal validity information whether the message is still valid.

[0019] According to a still other aspect of the present invention a software program product is provided implementing, when loaded into a computing device of a distributed system, a method according to anyone of the preceding claims.

[0020] According to a still other aspect of the present invention a distributed system for communicating authenticated data from an originator to a destination is provided. The system is designed for a keyed-hashing technique according to which data to be authenticated is concatenated with a private key and then processed with a cryptographic (one-way) hash function. The data are then transmitted together with the digest of the hash function from the originator to the destination. The data thereby comprised temporal validity information representing the temporal validity of the data.

[0021] The originator can be designed to define the temporal (limited) validity information.

[0022] The data can comprise random data which are unique for a time span defined by the temporal validity information.

[0023] The data can be a login key for a communication setup and/or a message.

[0024] According to a still other aspect of the present invention a distributed system for the authenticated transmission of messages is provided. The distributed system comprises an originator designed to generate a login key by a keyed-hashing method on the basis of random data, temporal validity information and a private key. Furthermore, a network for transmitting the login key from the originator to a destination is provided. The destination is designed to verify the authenticity and the temporal validity of the login key on the basis of the keyed-hashing digest.

[0025] The destination can be designed to generate an acknowledgement key by a keyed-hashing method on the basis of second random data and the private and to transmit the acknowledgement key to the originator in case the verification of the authenticity and the temporal validity of the login key is positive. The originator is designed to verify the acknowledgement key.

[0026] The acknowledgement key can furthermore comprise a time stamp and when verifying the acknowledgement key the originator checks on the basis of the time stamp and the temporal validity information whether the acknowledgement key is still valid.

[0027] The originator can be designed to extract the second random data from the acknowledgement key in case the verification of the acknowledgement key is positive, to generate the message by a keyed-hashing method on the basis of the second random data, message data and the private key and to transmit the message to the destination. The destination is designed to verify the message.

[0028] The message can furthermore comprise time stamp and when verifying the message, the destination checks on the basis of the time stamp and the temporal validity information whether the message is (still) valid.

[0029] Further features, advantages and objects of the present invention will become evident for the man skilled in the art when reading the following description of an embodiment taken in conjunction with the figures of the enclosed drawings.

Figure 1 shows hand shake and information flow between two communication partners with a time synchronised communication setup by keyed-hashing message authentication (TSCS),

Figure 2 shows the TSCS login key and acknowledgement key, and

Figure 3 shows the internal structure of a TSCS login key.

[0030] According to the time synchronised communication setup by keyed-hashing message authentication (TSCS) almost all setup keys are unique by using a secure random number generator. The setup key is only valid within a given time interval that is dynamically defined by the communication originator. The information sender and receiver authenticate each other. Only if both partners are authenticated, the information will be accepted by the communication partner. After the time interval is exceeded the setup key is invalid and cannot be reused again. Within the time interval the setup key can be reused. This feature is realised without storing of login keys.

[0031] The communication partners share only a single private (secret) key (of arbitrary length) which can be exchanged periodically using known secure protocols (e.g. a public key encryption method). The TSCS communication setup protocol is inherently robust against copy or replay attacks. As mentioned above, TSCS relies on the keyed-hashing for message authentication code (HMAC). It is known from the prior art that HMAC is hard to break even if the underlying secure hash function (e.g. SHA-1 or MD-5) has some weakness such as predictable collisions.

[0032] Figure 1 shows handshake and information flow between two communicating partners with the Time Synchronized Communication Setup by Keyed-Hashing Message Authentication (TSCS).

[0033] In phase 1 the information originator generates a TSCS login key and sends the login key to the receiver. As shown below a TSCS login key consists of a (secure) random bit array, a unified system time, a temporal validity field and its authentication key. If the random bit array is large the chance of generation of generating two identical random arrays is very small. The receiver receives the login key and checks its authentication key.

Because of the originator and the receiver share the same private key, the login keys digest differs if the login key has been altered (in this case further communication is denied). If the key is valid, the receiver checks its temporal validity as described in the validity field.

[0034] In phase 2 the receiver generates a TSCS acknowledgement key and sends it to the receiver. The acknowledgement key consists of a new random bit array (independent from the originator) and the unified system time of the receiver.

[0035] In phase 3 the originator checks the acknowledgement key (i.e. the digest and temporal validity), takes the random bit field of the acknowledgement key and merges it with the message data which is intended to be sent. The data (consisting of the message and the random field) is signed and sent to the receiver.

[0036] Then the receiver checks in phase 4 the message digest and the identity of random bit field (from the message) and the previously generated random bit array of the acknowledgement key. If the message digest is valid and the bit arrays are identical, the message has mot been altered AND was generated as a result of the previous exchange of login and acknowledgement keys. The receiver sends then an acknowledgement to the communication originator.

[0037] Figure 2 shows the TSCS login and acknowledgement key. The login key is created and signed by the communication originator. The acknowledgement key is returned and signed by the receiver. The transmitted signature is not necessarily the complete keyed-hashing message authentication code (HMAC) with its full digest length. For the login and acknowledgement keys it may be meaningful for security and key length to compress the digest to limit its length.

[0038] Figure 3 shows the internal structure of a TSCS login key. The HMAC key digest may be compressed to reduce key length and to prevent the private key K from key break attacks if the signed message is short (here 265 bit). A compression to 80 bit digest length (by a state machine) is appreciated for short message lengths.

[0039] The handshake between the two communicating parties consists of four phases. In the following the procedure according to the present invention will be explained in detail.

PHASE 1:

Communication originator login

[0040]

a) Generate a TSCS login key

b) generate of a secure random bit array
c) append the unified time (UT) field
d) append the temporal validity field
e) generate the Keyed-Hashing Message Authentication Code (HMAC) using private key K
f) append the HMAC (or a subset of) to the login key

g) transmit the login key to the receiver,

PHASE 2:

Receiver acknowledgement

[0041]

a) **[OPTION 1]** search the key table for a key that is identical to the current login key random bit field
b) **[OPTION 1]** if a duplicated key was found in the key table, terminate connection and exit.

c) **[OPTION 1]** store the random bit array of the login key in the key table until key expires

d) verification of the login key authenticity and validity

e) check the login key signature (the digest)

f) calculate own HMAC using private key K
g) compare own HMAC with login key digest

h) check the login key temporal validity

i) calculate the difference between login key universal time and current time (of the receiver).
j) check if time difference (the absolute value) is less then the temporal validity of the login key

k) generate the acknowledgement key

l) generate secure random bit array (the session key)
m) store session key
n) append the unified time (UT) field
o) generate the Keyed-Hashing Message Authentication Code (HMAC) using private key K
p) append the HMAC (or a subset of) to the acknowledgement key

q) transmit acknowledgement key to communication originator

PHASE 3:

Message transmission

[0042]

a) verification of the acknowledgement key authenticity and validity

b) check the acknowledgement key signature (the digest)

c) calculate own HMAC using private key K
d) compare own HMAC with acknowledgement key digest

e) check the acknowledgement key temporal validity

f) calculate the difference between acknowledgement key universal time and current time (of the originator).
g) check if time difference (absolute value) is less then the temporal validity of the acknowledgement key

h) extract the random bit field from acknowledgement key
i) append or merge the random field (the session key) with the message data
j) **[OPTION 2]** append universal time (of the originator) to the message
k) sign the message data and session key (and optionally universal time), i.e. calculate HMAC of message data and session key using private key K
l) append HMAC (or a subset of) to the message data and session key
m) transmit the message, i.e. transmit the message data, session key and HMAC to the receiver

PHASE 4:

Message verification

[0043]

a) verification of the message authenticity (and optionally validity)

b) compare the session key of the message with the previously stored session key
c) check the message signature (the digest)

d) calculate own HMAC using private key K
e) compare own HMAC with message digest
f) **[OPTION 2]** check the message temporal validity

g) **[OPTION 2]** calculate the difference between message universal time and current time (of the receiver) (optionally)
h) **[OPTION 2]** check if time difference (absolute value) is less then the temporal validity of the acknowledgement key (optionally)

i) return an acknowledgement to the communication originator

[0044] OPTION 1 is designed to eliminate so-called reply attacks (multiple use of the TSCS login key) even if the time span according to the appended temporal validity field is not yet expired. Note that said time span can be user defined between some nanoseconds and some minutes. Particularly in an Internet environment the time span will be chosen to be very long, wherein in direct connected networks it will be chosen to be quite short.

[0045] OPTION 2 gives the possibility to define a further time span for the temporal validity of the message itself.

[0046] As explained the invention relates to authenticated transmission of messages in distributed messaging and (multimedia) telecommunication systems. Time synchronized message and communication authentication can be also applied to a common message based communication between two communication partners. With minimal extension the TSCS can be also applied to 1-to-N communication like broadcast. The present invention relates to message oriented communication. Logically, message oriented communication means here that in an initial step the communication is established, then the message is send and in a third step an (optional) acknowledgement is returned by the receiving party. Message oriented communication is not effective for applications that require continuous (uni- or bi-directional) data transmission such as in real-time voice or video transmissions.

[0047] A technique for realizing secure authentication of communication setup and message transmission between two communicating parties is described. Time Synchronized Communication Setup by Keyed-Hashing Message Authentication (TSCS) provides the ability of

- Authentication of communicating partners.
- Authentication of transmitted information.
- Communicating partners share only a single private key that can be periodically changed (between the partners) by using state-of-the-art public key encryption for key transmission.
- Limited temporal validity (from nanoseconds to days) of session keys that enhances communication security and limits the chance and the effects of copy or replay attacks,

- Unsolicited message data sent from replay attacks will be (almost) detected,
- When secure random keys are stored during their time of validity (from nanoseconds to days), replay attacks during the initial communication setup phase (which does not harm message integrity) are (almost) impossible,
- Formerly exchanged session keys can (almost) never be reused again after a defined time interval (defined by the communication originator). This key property is realized without the storage of session keys.
- Limitation (inherent in the apparatus) of the temporal validity of transmitted information.

Claims

1. Method for the authentication of data communicated from a originator to a destination,
wherein a keyed hashing technique is used, according to which data to be authenticated is concatenated with a private key and then processed with a cryptographic hash function, and the data are transmitted together with the digest of the hash function from the originator to the destination,
characterized in that
the data comprises temporal validity information representing the temporal validity of the data.

2. Method according to claim 1,
characterized in that
the temporal validity information can be defined by the originator.

3. Method according to anyone of the preceding claims,
characterized in that
the data comprises random data which are unique for a time span defined by the temporal validity information.

4. Method according to anyone of the preceding claims,
characterized in that
the data is a login key for a communication setup and/or a message.

5. Method for the authenticated transmission of messages,
comprising the following communication setup steps:

   - generating a login key by a keyed-hashing method on the basis of random data, temporal validity information and a private key,
   - transmitting the login key from an originator to a destination, and
   - verifying the authenticity and the temporal validity of the login key on the basis of the keyed hashing digest on the destination side.

6. Method according to claim 5,
furthermore comprising the following acknowledgment steps:
in case the verification of the authenticity and the temporal validity of the login key is positive,

   - generating an acknowledgment key by a keyed-hashing method on the basis of second random data and the private key,
   - transmitting the acknowledgment key from the destination to the originator, and
   - verifying the acknowledgment key by the originator.

7. Method according to claim 6,
characterized in that
the acknowledgment key furthermore comprises a time stamp and when verifying the acknowledgment key it is checked on the basis of the time stamp and the temporal validity information whether the acknowledgment key is still valid..

8. Method according to claim 6 or 7,
furthermore comprising the following message transmission steps:
in case the verification of the acknowledgment key is positive,

   - extracting the second random data from the acknowledgment key,
   - generating a message by a keyed-hashing method on the basis of the second random data, message data and the private key,
   - transmitting the message from the originator to the destination, and,
   - verifying the message by the destination.

9. Method according to claim 8,
characterized in that
the message furthermore comprises a time stamp and when verifying the message it is checked on the basis of the time stamp and the temporal validity information whether the message is still valid.

10. Software program product,
characterized in that
it implements, when loaded into a computing device of a distributed system, a method according to anyone of the preceding claims.

11. Distributed system for communicating authenticated data from a originator to a destination,
designed for a keyed hashing technique according to which data to be authenticated is concatenated

with a private key and then processed with a cryptographic hash function, and the data are transmitted together with the digest of the hash function from the originator to the destination,
characterized in that
the data comprises temporal validity information representing the temporal validity of the data.

12. Distributed system according to claim 11, characterized in that
the originator is designed to define the temporal validity information.

13. Distributed system according to claim 11 or 12, characterized in that
the data comprises random data which are unique for a time span defined by the temporal validity information

14. Distributed system according to anyone of claims 11 to 13
characterized in that
the data is a login key for a communication setup and/or a message

15. Distributes system for the authenticated transmission of messages comprising:

- an originator designed to generate a login key by a keyed-hashing method on the basis of random data, temporal validity information and a private key.
- a network for transmitting the login key from the originator to a destination,

wherein the destination is designed to verify the authenticity and the temporal validity of the login key on the basis of the keyed hashing digest.

16. Distributed system according to claim 15 , wherein the destination is designed to generate an acknowledgment key by a keyed-hashing method on the basis of second random data and the private key and to transmit the acknowledgment key to the originator in case the verification of the authenticity and the temporal validity of the login key is positive, and
the originator is designed to verify the acknowledgment key.

17. Distributes system according to claim 16, characterized in that
the acknowledgment key furthermore comprises a time stamp and when verifying the acknowledgment key the originator checks on the basis of the time stamp and the temporal validity information whether the acknowledgment key is still valid..

18. Distributed system according to claim 16 or 17, characterized in that
the originator is designed to extract the second random data from the acknowledgment key in case the verification of the acknowledgment key is positive, generate a message by a keyed-hashing method on the basis of the second random data, message data and the private key, and transmit the message to the destination, and the destination is designed to verify the message.

19. Distributed system according to claim 18, characterized in that
the message furthermore comprises a time stamp and when verifying the message, the destination checks on the basis of the time stamp and the temporal validity information whether the message is still valid.

FIG 1

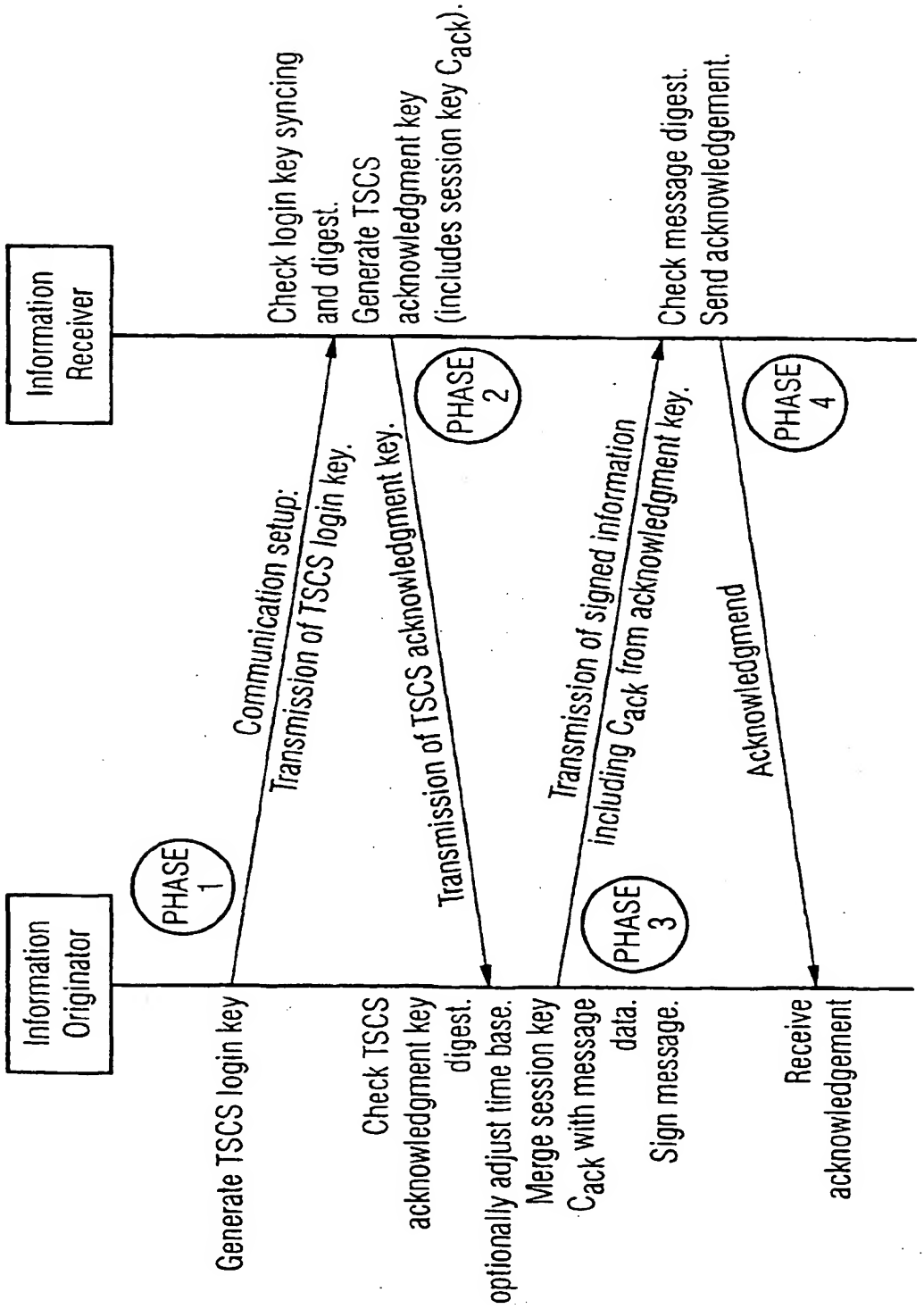


FIG 2

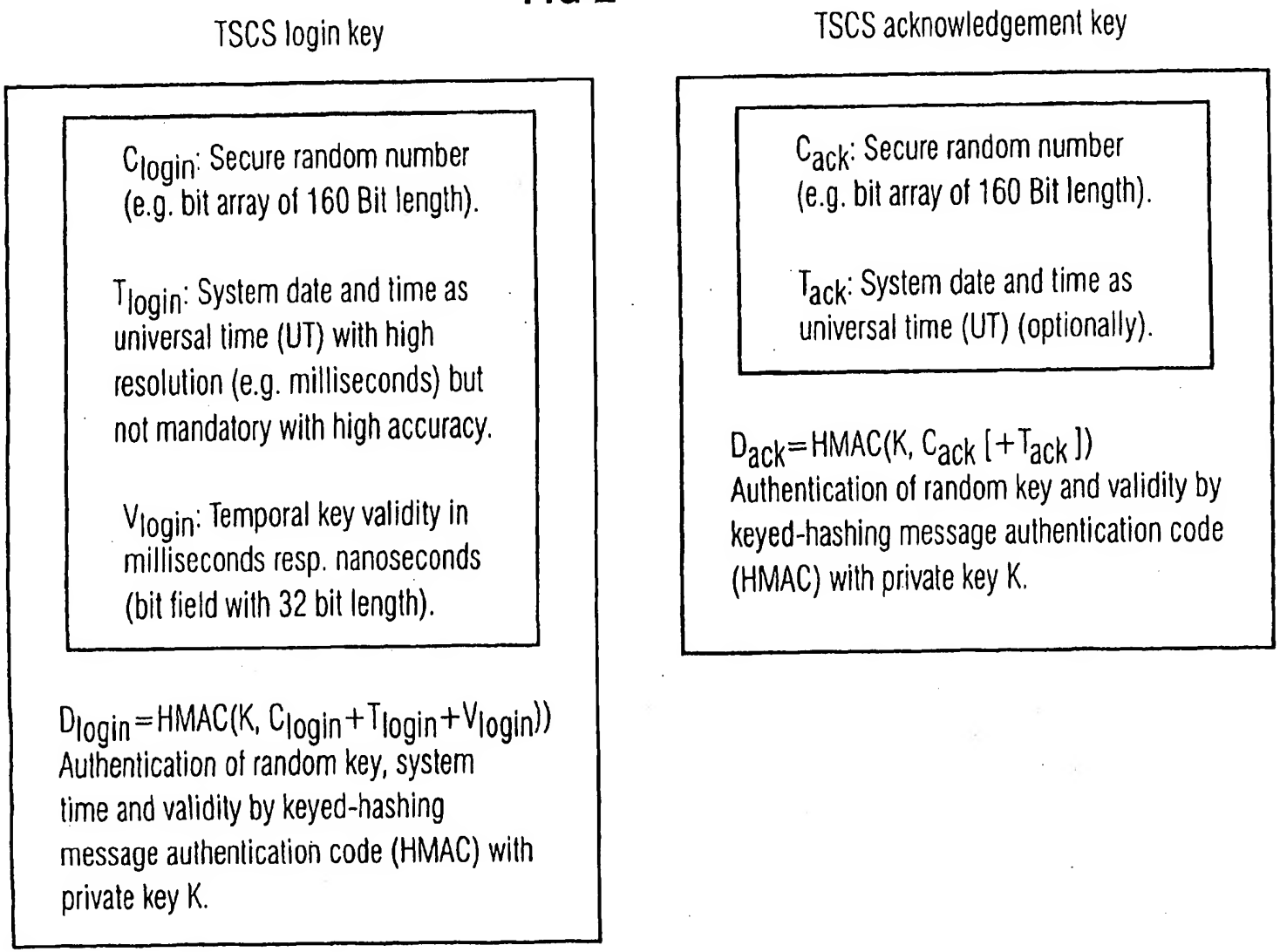
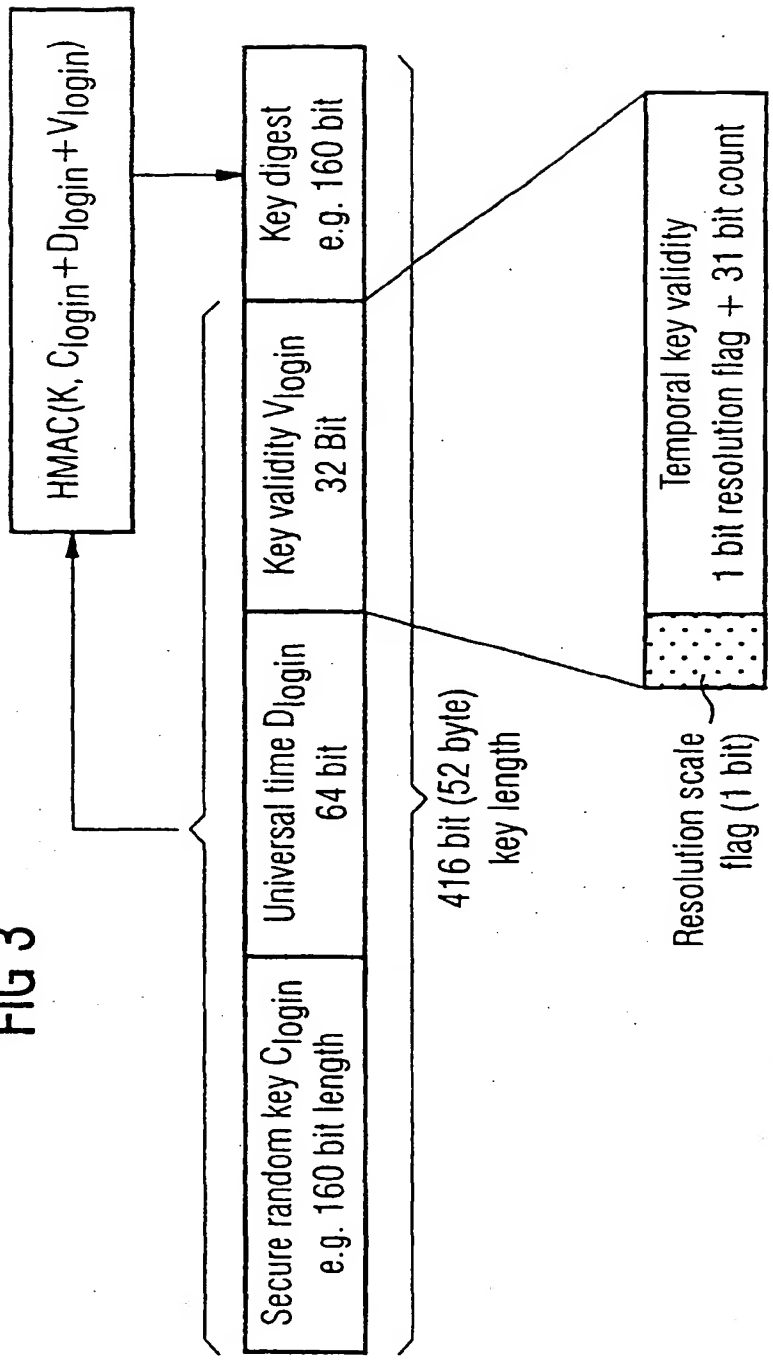


FIG 3



European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 12 4150

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X Y A	WO 99 57846 A (KYBERPASS CORP) 11 November 1999 (1999-11-11) * abstract * * page 8, line 8 - line 18 * * claim 1 *	1,2,4, 10-12,14 3,5,13, 15 6-9, 16-19	H04L9/32 H04L29/06
Y	US 5 926 549 A (PINKAS DENIS) 20 July 1999 (1999-07-20) * abstract *	3,5,13, 15	
A	EP 0 874 300 A (SONY CORP) 28 October 1998 (1998-10-28) * abstract * * page 26, line 3 - line 27 *	1,5,11, 15	
D,A	BELLARE M ET AL: "KEYING HASH FUNCTIONS FOR MESSAGE AUTHENTICATION" PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO),DE,BERLIN, SPRINGER, vol. CONF. 16, 1996, pages 1-15, XP000626584 ISBN: 3-540-61512-1 * page 1, paragraph 1 - page 2, paragraph 2 * * page 3, paragraph 6 - page 4, paragraph 1 * * page 5, paragraph 8 - page 6, paragraph 1 *	1,5,11, 15	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)
H04L
G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	18 May 2000	Blanco Cardona, P

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 12 4150

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

18-05-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9957846 A	11-11-1999	AU 3624599 A	23-11-1999
US 5926549 A	20-07-1999	FR 2744818 A	14-08-1997
		CA 2197266 A	13-08-1997
		EP 0800300 A	08-10-1997
EP 0874300 A	28-10-1998	JP 11053264 A	26-02-1999
		CN 1202658 A	23-12-1998
		CN 1202659 A	23-12-1998
		EP 0874299 A	28-10-1998
		JP 11055248 A	26-02-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82